Hardware Implementation of Genetic Algorithm Based Digital Colour Image Watermarking

S.Sreejith, N.Mohankumar, M.Nirmala Devi
Student, M-Tech VLSI Design, Asst. Prof., VLSI Design Research Group
Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Coimbatore, India
sreejith146@gmail.com, mk.mohankumar@gmail.com, m_nirmala@cb.amrita.edu

***Abstract*— The objective of this work is to develop a hardware-based watermarking system to identify the device using which the photograph was taken. The watermark chip will be fit in any electronic component that acquires the images, which are then watermarked in real time while capturing along with separate key. Watermarking is the process of embedding the watermark, in which a watermark is inserted in to a host image while extracting the watermark the watermark is pulled out of the image. The ultimate objective of the research presented in this paper is to develop low-power, high-performance, real-time, reliable and secure watermarking systems, which can be achieved through hardware implementations. In this paper the development of a very Large Scale Integration (VLSI) architecture for a high-performance watermarking chip that can perform invisible colour image watermarking using genetic algorithm is discussed. The prototyped VLSI implementation of watermarking is analyzed in two ways.**
Viz.,(i) Digital watermarking

***IndexTerms*—Digital watermarking, VLSI, Genetic algorithm, colour space transformation, Hardware Implementation**

I. INTRODUCTION

Digital data protection becomes a major issue. In the current scenario unauthorized replication and manipulation of digital content can be easily achieved using different tools. This is overcome by watermarking the digital content along the owner's key or with some logo. Watermark is the process of embedding a data, image in to the host image, video, and audio .This can be done in various domain. There are a lot approaches in software domain, and hardware domain according to applications. In general, watermarking consists of mainly two parts (1) watermark embedding (2) watermark detection [1]. Each owner has separate key that also included along with the original watermark. The key that helps not only for owner privacy but also to identify the watermark location during the detection. Watermarks can be embedded in different domain; spatial domain and frequency domain. Frequency domain method has more advantage compared to spatial domain like DCT domain watermarking. They are more robust and perceptible quality is also better. But the disadvantage is that, the circuit is more complex and hence the computational overhead is high. For spatial domain, watermarking is faster in terms of computational time and it is best suitable for real-time application. Hence the spatial domain approach is focused in this paper. This time domain watermarking is combined with genetic algorithm to achieve robustness.

According to perceptual quality of image digital watermarking can be divided in to three types visible, invisible and dual. Visible watermarking is perceptible to naked eye just like logo inserted in to a corner of an image. Invisible watermarking is percentile to human eye. A dual watermarking is combination of visible and invisible watermark. Invisible and visible watermarking further classified as robust and fragile. For copyright protection, this kind of watermarks are utilized. Fragile watermarks are embedded in such a way that any modification or manipulation of the host image would corrupt the watermark. Therefore, fragile watermarks are mainly used for authentication purposes.

Genetic algorithm is based on the nature's selection law "survival of the fittest". Different steps of genetic algorithm are initializing the population, selection, crossover, mutation and fitness value calculation. Genetic algorithm is suitable for problems like optimization and search space evaluation [3]

The rest of the paper is organized as follows: section II highlights the contribution of this paper. Section III deals with the previous work and literature survey result, section IV describes the explanation of algorithm used in this paper, section V describes the designing of the proposal, section VI includes the results and then conclusion.

II. CONTIRBUTION OF THIS PAPER

Here a hardware implementation of genetic algorithm based invisible robust watermarking for colour image has been proposed. The approach used for designing the watermark embedding is in time domain. The genetic algorithm is used here for finding a search space and optimizing the intensity to best fit for the watermark image. Most of the previous work use pseudorandom number as watermark. But in this proposal we are going to use another image with intensity {0,1,2} is used along with key as watermark. For colour image watermarking RGB is converted to YUV and watermark is done at Y channel. The designed architecture is to be implement as custom IC [7]. The proposed watermarking camera as shown in Figure.1 can be fit in to any electronic media.

The image sensor and the analog to digital convertor produce the digital colour image. Then the colour image is stored in a temporary memory. For separating the

DOI: 01.IJSIP.02.01.71

luminance channel (i.e.) Y channel the colour space transformation is used. RGB to YUV conversion block converts the colour image to YUV. Then watermarking is done in the Y channel. One of the two LSB bits of Y channel is embedded with watermark image bit and the other bit is complement of the watermarked bit. It will helps at the time of detection by comparing the two bits. Here invisible robust watermarking is used after the embedding operation the image is converted to RGB format and stored in to the flash memory of the camera. By using control signal from the control block,it is controlled. LCD panel is used to display the colour image or watermarked image, that will be determined by the control signal. Genetic algorithm is used to determine the dark or bright pixels in the host image that is similar as the watermark image for getting a invisible watermark image. Each section is explained in section IV and V.

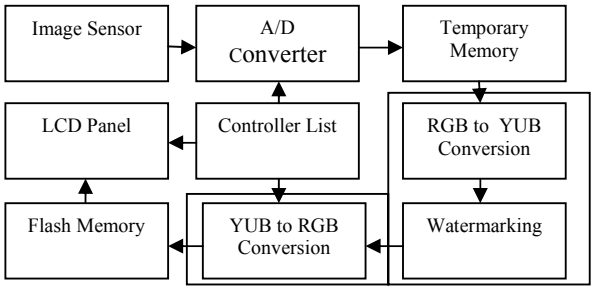

Figure.1 Architecture of digital Camera with watermarking capability

III. RELATED WORK

Various types of watermarking algorithms developed for different type of media, such as image, video, audio and text data. The watermarking is already implemented in various domains like spatial ,DCT , and wavelet. All these works focus on software implementation. So there is a gap between image capture and image transmission. Hence it is not suitable for real time application. Hardware implementation is attempted here to overcome the drawback (i.e.) it is best suitable for real time applications

Tsai and Lu [8] propose a DCT domain watermarking Chip. The watermarking system embeds a pseudorandom sequence of real numbers. The chip is implemented with TSMC 0.35 µm technology and has a die size of 3.064× 3.064 mm^2 and 46,374 gates. The chip is estimated to consume 62.78 mW of power when operated at 50MHz frequency with a 3.3V supply.

Mohanty et al.[2] propose a visible watermarking algorithm and implemented as a custom IC. The proposed architecture have implemented in two ways (1) pixel by pixel (2) block by block. The chip implemented in 0.35 µm technology. The chip die size is 3.34×2.89 mm^2 it works at a frequency of 292 MHz, the supply voltage is 3.3V and obtained power is 6.93 mW.

Mohanty et al.[1] propose another watermarking algorithm for Invisible robust and invisible fragile model. The work implemented in spatial domain. The chip is implemented in 0.35 µm technology. The chip die size is15.012 × 14.225mm^2 . The chip works at 545 MHz with supply voltage , 3.3V which consumes a power of 2.0547 mW

Garimella et al [12] propose a VLSI architecture for invisible-fragile watermarking in spatial domain. In this scheme, the differential error is encrypted and interleaved along the first sample. The watermark can be extracted by accumulating the consecutive Least Significant Bits(LSBs) of pixels and then decrypting. The extracted watermark is then compared with the original watermark for image authentication. The ASIC is implemented using 0.13 µm technology. The area of the chip is 3453×3453mm^2 and consumes 37.6 uW power when operated at 1.2 V . The critical path delay of the circuit is 5.89ns.

Annagirao Garimella et.al.[7] proposed ASIC for colour image watermarking. In this colour space transformation algorithm is used to convert RGB to YUV transformation. Then the watermarking is done in the first LSB of Y channel.

Shian-De Chen et.al.[3] proposed a genetic algorithm chip. Which has flexibility for selecting the fitness value, so it is best suitable for real time application.

Table 1.
Summary of the Previous Works

Work	Type	Object	Domain	Chip statistics
Hyan Lim , Wan-Hyun [9]	Invisible	Grey scale image	DCT	ALTERA flex family FPGA 50mHz
Tsai and Lu[8]	Invisible Robust	Grey scale image	DCT	0.35um, 3.0x3.0 mm , 3.3v,50MHz,62.7mW
Garimella et.al.[11]	Invisible fragile	Grey scale image	spatial	*0.13um, 3.453 x3.453 mm^2 ,1.2V , 100MHz, 37.6uW*
Mohanty ,et . al. [2]	Visible	Grey scale image	spatial	*0.35um, 3.34X 2.89mm^2 3.3V , 292MHz,6.93mW*
Mohanty ,et . al. [1]	Invisible robust & fragile	Grey scale image	spatial	*0.35um, 3.3V , 15.012 x 14.225mm2, 545MHz, 2:0547mW*

IV. ALGORITHMS

Different algorithms used in this works are (A) Invisible robust watermarking [1] (B) Modified Genetic algorithm [3] (C) RGB-YUV transformation algorithm [7].

A. Invisible Robust watermarking [1]

The algorithm works in spatial domain. It can withstand various major attacks like image processing attack and geometric attack.

The watermarking insertion process is explained with the help of Figure 2. The watermark image *W* is ternary image (a three level grey scale image) with pixel value {0,1,2}. The insertion process is explained in the following algorithm . The initial insertion sequence is *K*

DOI: 01.IJSIP.02.01.71

$$I_W(i,j) = \begin{cases} I(i,j) & \text{if } W(i,j) = 0 \\ E_1[I(i,j), I_N(i,j)] & \text{if } W(i,j) = 1 \\ E_2[I(i,j), I_N(i,j)] & \text{if } W(i,j) = 2 \end{cases} \quad (1)$$

E_1 and E_2 are the encoding function, Iw is the watermarked image. The encoding function E_1 and E_2 are the function of original image I (i,j) and its neighborhood image $I_N(I,j)$.The encoding functions are

$$\begin{aligned} E_1(I, I_N) &= (1-\alpha_1) I_N(i,j) + \alpha_1 I(i,j), \\ E_2(I, I_N) &= (1-\alpha_1) I_N(i,j) - \alpha_2 I(i,j), \end{aligned} \quad (2)$$

Where α_1, α_2 and (1- α_1) are the scaling factors. α_1 and α_2 is used to scale the original watermark data $I(i,j)$ and (1- α_1) is used to scale the neighborhood image data $I_N(I,j)$ to ensure that the watermarked image intensity value does not exceed the maximum 8-bit value (i.e.) 255.which satisfy the condition $0< \alpha_1<1$ and $-1< \alpha_1<0$.

For finding the neighborhood image data, first set an smallest neighborhood radius and find the average of the neighborhood images.

$$I_N(i,j) = \frac{1}{3}\{I(i+1,j) + I(i+1,j+1) + I(i,j+1)\}. \quad (3)$$

Division by three makes the hardware implementation difficult. In this algorithm it is rearranged it as

$$I_N(i,j) = \left\{ \frac{\frac{I(i+1,j)+I(i+1,j+1)}{2} + I(i,j+1)}{2} \right\}. \quad (4)$$

It is simplified by division by two to implement in hardware. A division of two is implemented as one-bit right shift operation.

B. Modified Using Genetic algorithm[3][5][6]

Genetic Algorithm is used to find out the optimum intensity value in the host image that is best suitable for the watermark image intensity. (i.e) for dark intensity of the watermark images the genetic algorithm will find out a similar intensity in the host image, to attain an invisible watermarking. It will simply find the neighborhood data around the neighborhood radius *r*. Genetic algorithm will search and find out an optimum intensity region and watermarking is done using these optimum value as neighborhood value and encoding done with the help of encoding function E_1 and E_2 . Then the above algorithm repeats. i.e. Encoding is done with the help of the equation.(1).

C. RGB-YUV colour space transformation algorithm[7]

In this algorithm, the first step is to convert the RGB component of colour image to YUV. Y channel is the luminance channel. Once RGB is converted in to YUV, then using the above two procedure ((A),(B)), the watermarking is possible. In this algorithm the two lower bit of Y-channel is watermarked , in the first bit the watermark data and in the next bit the complement of the first bit data. The advantage of this method is that we can recover the original watermark without the knowledge of original image $I(i, j)$. The algorithm is follows, first the colour space transformation it can achieve using the equation (6). The general formula for colour space transformation is

$$\begin{bmatrix} S_1' \\ S_2' \\ S_3' \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ S_3 \end{bmatrix} \quad (5)$$

Where $[S_1 \ S_2 \ S_3]^T$ is the original colour space and $[S_1' \ S_2' \ S_3']^T$ is the transformed colour space.

The equation (6) transforms the gamma corrected RGB to YUV space

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (6)$$

V.HARDWARE IMPLEMENTATION

A. Invisible Robust Watermarking

The watermark image is generated either with the help of LFSR or 128X128 image given through D_in and stored in to Watermark RAM. The host image has 256X256 pixel that is store in to host image RAM using address decoder (Addr Decoder) and data_sel. Using Adder1 and Adder2 this algorithm will generate the neighborhood values. The multiplier unit will generate the two encoding function. According to the pixel value coming from the watermark RAM The MUX4X1 unit select the encoding function (Equation.1) and replace the corresponding values in the host image RAM. Thus Watermarked image is generated as shown in Figure 2

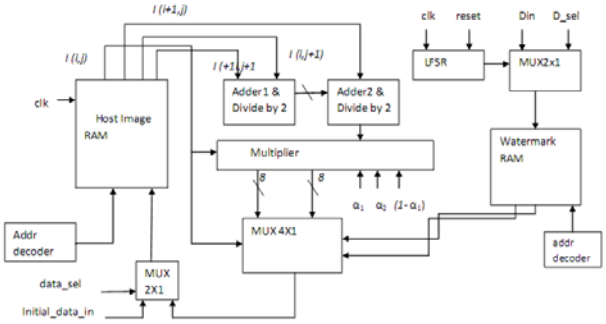

Figure 2 . Invisible Watermarking architecture

B. Genetic Algorithm

In this work, the main focus is on hardware implementation of genetic algorithm. A flexible genetic algorithm processor is implemented. The main advantage of this processor is that it can perform dynamically various fitness function four crossover operations, and over ten thousand kinds of mutation-rate settings to meet the requirements of different applications. This proposed architecture is very useful for real-time applications.Genetic algorithm have six main blocks :

DOI: 01.IJSIP.02.01.71

population initialization, fitness calculation, termination judgment, selection, crossover, and mutation [3].

VI. SYNTHESIS RESULT

The design of full Colour image watermarking is completed. We checked the watermarking with the help of binary image using Precision Synthesis 2008a.47, ModelSim 6.4c and Altera quartus 9 version. The synthesis result is tabulated in Table 2&3. The Result tabulated here is only a part of this work. The code is not Optimized for low power.

Table 2
Timing & power analysis Report
(Target device : Altera Cyclone ii Family)

Clock Speed	5ns
Input Delay	3ns
Output Delay	1ns
Slack	5.753ns
Static Power Dissipation	47.36mW
Thermal Power Dissipation	73.84mW

Table 3
Area Report

Altera Family (Cyclone ii)	EP2C20F484C7
System Requirements	Intel Core2Duo processor,2 GB RAM
Total Logic Elements	2672
Total Registers	2048

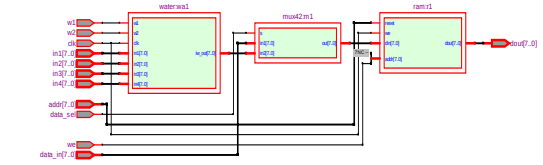

Figure 3 . RTL view of watermarking Algorithm

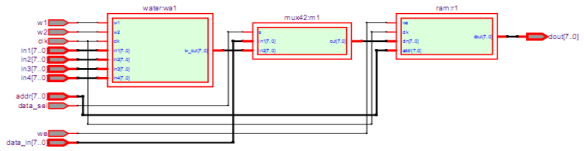

Figure 4. Watermark module

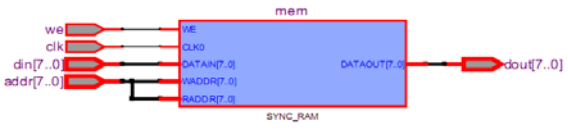

Figure 5. RAM Module

VII .CONCLUSION

In this paper we propose a hardware architecture for digital colour image watermarking. The hardware implementation of binary image watermarking algorithm is completed. The full flow of colour image watermarking is completed. In this work mainly focusing the colour image watermarking. This watermarking design is done in spatial domain and genetic algorithm is integrated with this module to achieve flexibility selection and robustness of the watermarked image. Future enhancement is to reduce the power dissipation and area.

REFERENCES

[1] Mohanty, S.P. Kougianos, E. Ranganathan, N. "*VLSI architecture and chip for combined invisible robust and fragile watermarking*" : *Computers & Digital Techniques, IET Publication Sept. 2007, 10.1049/iet-cdt:20070057*

[2] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S2DC) Design," *IEEE Transactions on Very Large Scale Integration Systems (TVLSI), vol.* 13, no. 8, pp. 1002–1012, August 2005.

[3] Shian-De Chen, Pei-Yin Chen and Yung-Ming Wang, "A Flexible Genetic Algorithm Chip**"**

[4] Sheng-Kai Song, Wei-Ming Li, and Li Song"*Digital Watermark-Based Trademark Checker*", *http://www.altera.com/literature/dc/lit-design-contest.jsp*

[5] Jialing Han1,2, Jun Kong1,2, Yinghua Lu1, Yulong Yang1, and Gang Hou1,3, "A Novel Colour Image Watermarking Method Based on Genetic Algorithm and Neural Networks", *Springer-Verlag Berlin Heidelberg 2006*

[6] Chen Yongqiang,Peng Lihua, "Optimal Image Watermark Using Genetic Algorithm and Synergetic Neural Network**"** *Second International Conference on Intelligent Computation Teclmology and Automation 2009*

[7] Annajirao garimella, M.V.V satyanarayana, P.S. Murugesh, U.C. Niranjan "ASIC For Digital Colour image Watermarking" *11 th Digital Signal Processing Workshop and IEEE signal Processing Education Workshop*2004 IEEE

[8]. T. H. Tsai and C. Y Lu, "A Systems Level Design for Embedded Watermark Technique using DSC Systems*," in Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems, 2001.*

[9] Hyun Lim, Soon-Young Park and Seong-Jun Kang, Wan-Hyun Cho," FPGA Implementation of Image Watermarking Algorithm for a Digital Camera*", IEEE Transactions on Very Large Scale Integration Systems IEEE 2003.*

[10] *Digital Watermarking and Steganography Fundamentals andTechniques*,FrankYShih.

DOI: 01.IJSIP.02.01.71